RGC Ref. No.:
UGC/FDS14/E03/16
(please insert ref. above)

RESEARCH GRANTS COUNCIL
COMPETITIVE RESEARCH FUNDING SCHEMES FOR
THE LOCAL SELF-FINANCING DEGREE SECTOR

FACULTY DEVELOPMENT SCHEME (FDS)

Completion Report
(for completed projects only)

Submission Deadlines:
1. *Auditor's report with unspent balance, if any: within **six** months of the approved project completion date.*
2. *Completion report: within **12** months of the approved project completion date.*

Part A: The Project and Investigator(s)

1. Project Title

Secure Cloud Database System using Communication-Efficient Multi-Party Computation

2. Investigator(s) and Academic Department(s) / Unit(s) Involved

Research Team	Name / Post	Unit / Department / Institution
Principal Investigator	Dr. Wong Wai Kit Assistant Professor	Department of Computing The Hang Seng University of Hong Kong
Co-Investigator(s)	Prof. Cheung Wai-lok, David Professor	Department of Computer Science The University of Hong Kong
Others		

3. Project Duration

	Original	Revised	Date of RGC / Institution Approval *(must be quoted)*
Project Start Date	1 Jan 2017	1 Jan 2017	
Project Completion Date	31 Dec 2019	30 Jun 2020	19 Jul 2019
Duration *(in month)*	36	42	19 Jul 2019

Deadline for Submission of Completion Report	31 Dec 2020	30 Jun 2021	19 Jul 2019

Part B: The Final Report

5. Project Objectives

5.1 Objectives as per original application

1. Use existing operators in multi-party secret sharing model to construct a cloud database system that supports basic query processing.

2. Extend the functionality of the cloud database system with new operators, including but not limited to text operators (e.g., like operator).

3. Develop database optimization techniques, e.g., indexing, that can be executed in multi-party secret sharing model.

4. Develop communication-efficient techniques and apply them in the operators of cloud database system.

5. Prove the security of developed algorithms/protocols.

6. Perform theoretical and empirical analysis on the performance of the developed database system and compare it with other secure cloud relational database systems.

5.2 Revised objectives

N/A

Date of approval from the RGC: _____

Reasons for the change: _____

_____

1.

2.

3. ....

5.3 Realisation of the objectives

(Maximum 1 page; please state how and to what extent the project objectives have been achieved; give reasons for under-achievements and outline attempts to overcome problems, if any)

Objective 1. Use existing operators in multi-party secret sharing model to construct a cloud database system that supports basic query processing.

In the last report, we were more or less done for this objective except that we planned to support operations on non-numeric data. In the end, we decided to use and develop bit-level operators to serve as building blocks for different kinds of operators. The reasons are that (1) more operators can be covered; and (2) the concern on the overhead of composing low-level operators to form higher-level operators is addressed by the optimized algorithms (see objective #4.

Objective 2. Extend the functionality of the cloud database system with new operators, including but not limited to text operators (e.g., like operator).

This is supported by using bit-level operators.

Objective 3. Develop database optimization techniques, e.g., indexing, that can be executed in multi-party secret sharing model.

Indexing can be done using the bit-level building blocks.

Objective 4. Develop communication-efficient techniques and apply them in the operators of cloud database system.

Optimizations are done in two levels. First, we have successfully developed new algorithms to serve as the building blocks in our system that have lower computation and communication costs than existing methods. Second, we adopt a caching policy in our system. The idea is simple. When the primitive building blocks are repeated executed, it is often that the same message is required to be sent from one party to another. Instead of regenerating the encrypted version of this message (to achieve the best security), we allow to reuse the previous message in the new round of communication to save the communication overhead.

Objective 5. Prove the security of developed algorithms/protocols.

The proofs of all building blocks algorithms are done in the project.

6. Perform theoretical and empirical analysis on the performance of the developed database system and compare it with other secure cloud relational database systems

We have done 2 sets of experiments. (1) Experiments on the individual primitive building blocks; and (2) Experiments on applications using the building blocks. The first set of experiments is rather standard. We looked for state-of-the-art algorithms for individual operations and compare their performance. In the second set of experiments, we worked on a number of applications, including deep learning, data analytics, and robot search (no

requirement on security is enforced). In general, the experiments prove the efficiency of our developed methods.

5.4 Summary of objectives addressed to date

Objectives *(as per 5.1/5.2 above)*	**Addressed** *(please tick)*	**Percentage Achieved** *(please estimate)*
1. Use existing operators in multi-party secret sharing model to construct a cloud database system that supports basic query processing.	√	100%
2. Extend the functionality of the cloud database system with new operators, including but not limited to text operators (e.g., like operator), date and time operators (e.g., extracting the month of a timestamp), conversion operators (e.g., text-to-numeric conversion).	√	100%
3. Develop database optimization techniques, e.g., indexing, that can be executed in multi-party secret sharing model.	√	100%
4. Develop communication-efficient techniques and apply them in the operators of cloud database system.	√	100%
5. Prove the security of developed algorithms/protocols	√	100%
6. Perform theoretical and empirical analysis on the performance of the developed database system and compare it with other secure cloud relational database systems.	√	100%

6. Research Outcome

6.1 Major findings and research outcome
(Maximum 1 page; please make reference to Part C where necessary)

1. Bit-level operation for general functionality

While we planned in the proposal to develop customized algorithms for individual operators, we are able to identify and develop bit-level operators that serve as building blocks for supporting different operators. For instance, substring matching (text operator) can be viewed as a sequence of character (byte) comparisons. By developing a (byte) comparison operator, we are able to support this operation. In addition, comparison between image can be supported at bit-level. To be specific, we need bit-level operations like and/or/not and comparisons (equality and range comparisons). The challenge here is have a unified scheme that can represent the data securely and perform the aforementioned operations efficiently. We developed such a scheme in this project. We can compare our scheme to state-of-the-art algorithms for individual tasks, such as equality and range comparisons. Experiments showed that our scheme outperforms the state-of-the-art methods in terms of both computational and communication costs. The results imply that our scheme is not only suitable for our original designated application of secure database applications, but is also potentially valuable to be used in other applications for improvements.

2. Application in secure data analysis

   As one of the applications, we applied our methods in (big) data analytics. We used our developed building blocks to build a secure data mining algorithm. To be specific, we replace the primitive operators in a state-of-the-art clustering algorithm by using our building blocks. The computation and communication costs are reduced without further fine-tuning the algorithm. A manuscript about this application was prepared but is still not accepted to publish as of now.

3. Application in robot communications

   As another application, we do not necessarily apply the optimization ideas in security applications. In this case, we applied the optimization ideas in robot communications. A journal paper and a conference paper were published.

6.2 Potential for further development of the research and the proposed course of action *(Maximum half a page)*

Results for research outcomes 1 and 2 are not yet published. We submitted the manuscripts about the results but were not successful. As the PI has left academia, the publication work is now ceased.

7. **Layman's Summary**
   (Describe in layman's language the nature, significance and value of the research project, in no more than 200 words)

   The project aims to develop techniques for supporting cloud database systems using multi-party computation approach. The idea is to have multiple service providers collaboratively provide the function instead of a single service provider. The purpose is that no party becomes the single point of failure in terms of security. Efficiency and communication overheads are the keys to the project as communication between multiple parties can be complicated sometimes. In this project, we developed several building blocks for the project goal, e.g., secure equality check and range comparison operators. We can use these building blocks for not only database operations but also the more complicated data analysis among multiple parties. Experiments showed that our developed algorithms are more efficient than state-of-the-art competitors.

Part C: Research Output

8. **Peer-Reviewed Journal Publication(s) Arising Directly From This Research Project**
(Please attach a copy of the publication and/or the letter of acceptance if not yet submitted in the previous progress report(s). All listed publications must acknowledge RGC's funding support by quoting the specific grant reference.)

The Latest Status of Publications				Author(s) *(denote the corresponding author with an asterisk*)*	Title and Journal / Book *(with the volume, pages and other necessary publishing details specified)*	Submitted to RGC *(indicate the year ending of the relevant progress report)*	Attached to this Report *(Yes or No)*	Acknowledged the Support of RGC *(Yes or No)*	Accessible from the Institutional Repository *(Yes or No)*
Year of Publication	**Year of Acceptance** *(For paper accepted but not yet published)*	**Under Review**	**Under Preparation** *(optional)*						
2020				Wai Kit Wong, Shujin Ye, Hai Liu & Yue Wang	Effective Mobile Target Searching Using Robots. *Mobile Networks and Application.* (2020). https://doi.org/10.1007/s11036-020-01628-x	No	Yes (Annex I)	Yes	Yes

9. **Recognized International Conference(s) In Which Paper(s) Related To This Research Project Was / Were Delivered**
(Please attach a copy of each conference abstract)

Month / Year / Place	Title	Conference Name	Submitted to RGC *(indicate the year ending of the relevant progress report)*	Attached to this Report *(Yes or No)*	Acknowledged the Support of RGC *(Yes or No)*	Accessible from the Institutional Repository *(Yes or No)*
Nov / 2019 / Shenzhen, PRC	Search Planning and Analysis for Mobile Targets with Robots	EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness 2019	Nil	Yes (Annex II)	Yes	Yes

10. **Whether Research Experience And New Knowledge Has Been Transferred / Has Contributed To Teaching And Learning**
(Please elaborate)

The research assistant is new to the research area of this project. It takes a while to educate the research assistant to understand the project background. The learning experience allowed us to identify some potential difficulties in understanding machine communications and collaborations, e.g., why is it important and hard for machines to collaboratively work on a common goal? Such learning experience can be brought to the classroom as examples for sharing and provides some general guidelines for learning related problems, e.g., realizing the problem of machine communications using role play.

11. **Student(s) Trained**
(Please attach a copy of the title page of the thesis)

Name	Degree Registered for	Date of Registration	Date of Thesis Submission / Graduation
N/A			

12. **Other Impact**
(e.g. award of patents or prizes, collaboration with other research institutions, technology transfer, teaching enhancement, etc.)

Nil

13. **Statistics on Research Outputs**

	Peer-reviewed Journal Publications	Conference Papers	Scholarly Books, Monographs and Chapters	Patents Awarded	Other Research Outputs (please specify)	
No. of outputs arising directly from this research project	1	1	0	0	Type	No.

14. **Public Access Of Completion Report**
(Please specify the information, if any, that cannot be provided for public access and give the reasons.)

Information that Cannot Be Provided for Public Access	Reasons
Nil	